Design and Analysis of Recoverable Flight Control Systems for Harsh Environments[†]

W. Steven Gray **Oscar R. González**
Department of Electrical and Computer Engineering
Old Dominion University
Norfolk, Virginia USA

NASA Aviation Safety Technical Conference
October 22, 2008

[†] This work supported by the NASA Langley Research Center under grant NNX07AD52A.

Contents

1. Motivation and Research Objectives

- EM disturbances from natural/man-made sources can change data values on digital buses/memory and CPU instruction execution.
- Atmospheric neutrons passing through solid-state devices can cause single-event upsets (SEU's).
- SEU's are soft errors, i.e., they are transient and nondestructive to the hardware. Their effects have only been studied at the chip level.
- Both types of upsets can degrade the quality of the control signal and have an aggregate effect on closed-loop performance.

Research Objectives

- To develop tractable hybrid models of distributed flight control systems integrating the appropriate features of the fault-tolerant computing platforms and communication system.
- To analyze the corresponding flight control system performance degradation caused by High Intensity Radiated Fields (HIRF) environments and atmospheric neutrons.
- To develop a design methodology for distributed flight control systems that takes advantage of the fault-tolerant communication system services and mitigates the effects of digital upsets.
- To validate the effectiveness of a designed distributed/recoverable flight control system in three environments:
  - simulated hazardous environments
  - HIRF environments
  - neutron environments.

2. Hypothesis, Milestones and Technical Plan

Primary Hypothesis

Computationally distributed flight control systems using robust communication networks and recoverable computing platforms provide practical, predictable and superior control performance in harsh environments.

Relevant IVHM Milestones[†]

1.2.4.1 *Validated models of flight computer component failure, damage characterization, damage mitigation, and impact on flight safety.*

1.3.4.1 *Implement and benchmark algorithms to support reconfiguration, recovery, and redundancy management.*

[†] ASP IVHM Technical Plan, Version 2.0

2.1.2.1 *Validated methodologies and tools for the diagnosis of failures associated with aircraft components and subsystems implicated by the adverse events.*

2.1.3.1 *Validated methodologies and tools for the prognosis of failures associated with aircraft components and subsystems implicated by the adverse events.*

2.1.4.1 *Mitigation of flight computer and actuator failures and damage, and recovery from transient effects on flight computers with complex architectures, smart sensors, and actuators.*

3.4.1 *Establishment of minimum performance criteria of candidate mitigation strategies at the subsystem or component level for selected conditions.*

Technical Plan

Phase 1: System Design Which distributed control architectures are inherently the most reliable and give the best control performance in harsh environments?

Phase 2: Performance Models and Prediction Synthesize predictions of closed-loop performance for specific HIRF and neutron environments.

Phase 3: Test in Simulated Hazardous Environments Using a ROBUS-2 implementation of the best design, inject fault patterns to simulate HIRF and neutron environments.

Phase 4: Test in a HIRF Environment Test implementation in HIRF chamber at LaRC.

Phase 5: Test in a Neutron Environment Test implementation in neutron beam at Los Alamos Neutron Science Center.

3. Technical Progress

3.1 Design and Analysis Methods

Objective: Identify a specific network topology for a distributed/ recoverable flight control system which gives the best closed-loop tracking performance when random upsets are injected into the computing platform.

- Each processing unit is recoverable within one control cycle.
- The same control law is replicated on each processing element.
- Each processing element is fail-silent with 100% coverage.
- A voter determines the actual control command applied and is not subject to upset.
- Inject i.i.d. upset disturbances into all processing elements.
- Use a linearized Boeing 747 model with a straight/level flight control law and subject to light Dryden wind gusts (1 ft/sec).

An Illustrative Example

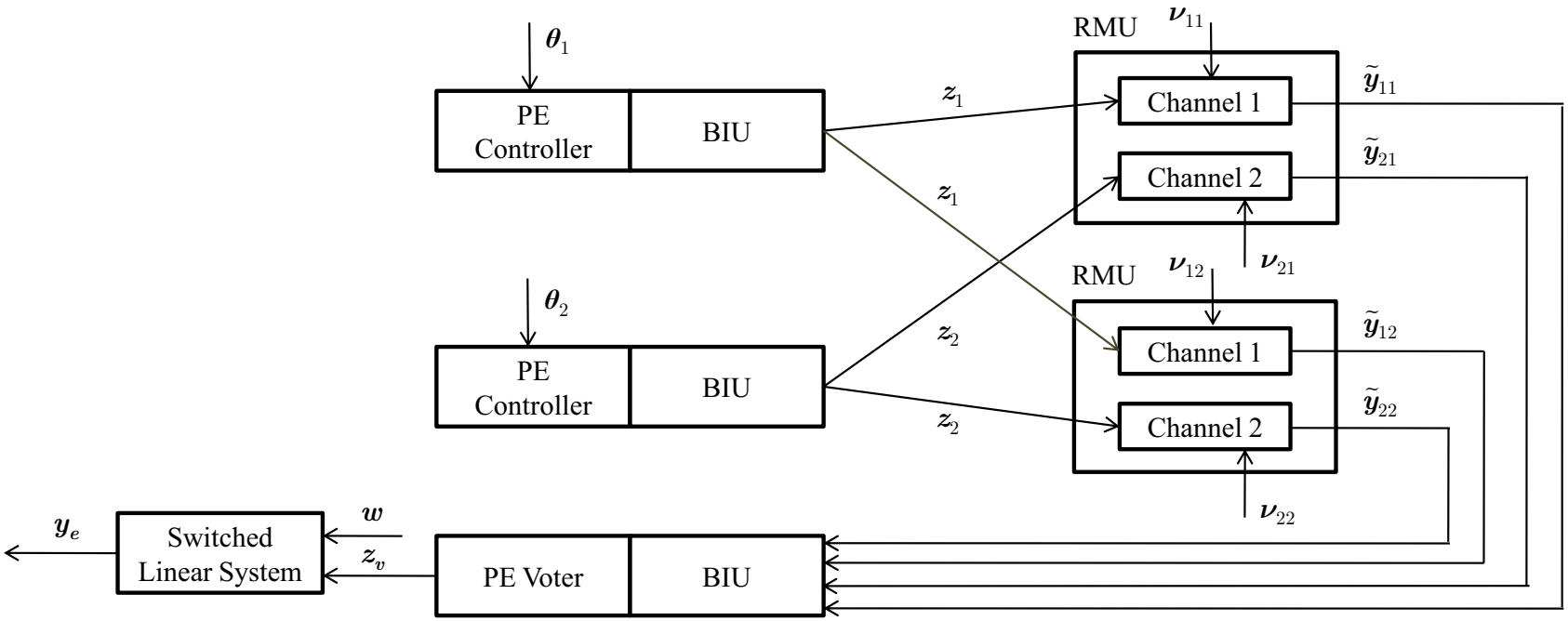

Fig. 1: Dual Processor Element (PE) platform with dual Redundancy Management Units (RMU's). Bus Interface Units (BIU's) connect the PE's to the communication system.

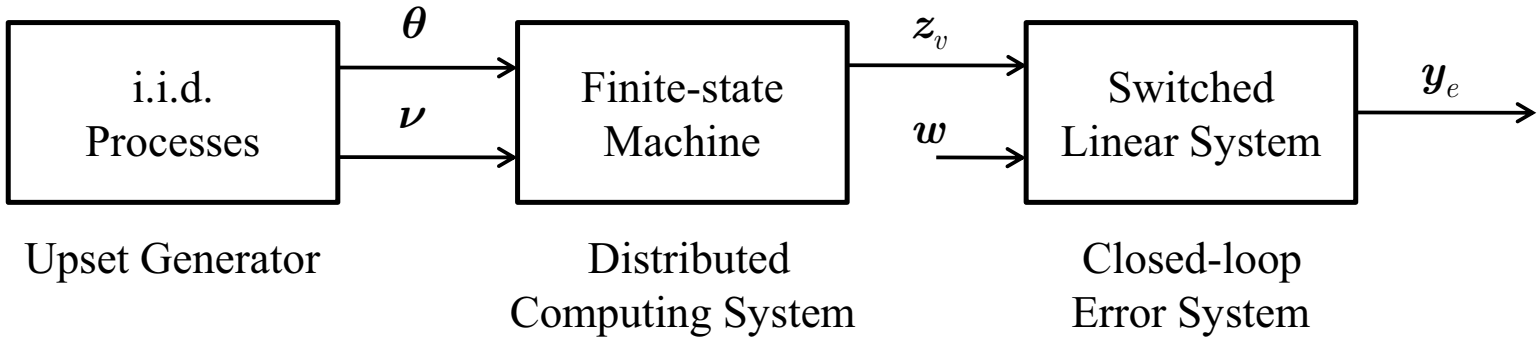

Fig. 2: A conceptual view of the performance model for the distributed flight control system.

The performance index of interest is the mean power in the output tracking error

$$J_w = \lim_{k \to \infty} E\{\|\boldsymbol{y}_e(k)\|^2\}.$$

To compute J_w analytically it is essential to understand the statistical nature of the voter output $\boldsymbol{z}_v(k)$.

What is known at present about the stochastic nature of the communication model:

- Internal states, e.g., $\boldsymbol{z}_i(k)$, are first-order homogeneous Markov processes.
- The inputs to the voter, $\tilde{\boldsymbol{y}}_{ij}(k)$, and the voter output, $\boldsymbol{z}_v(k)$ are not in general Markov processes.
- For the class of upset disturbances under consideration, however, these process are well approximated by homogeneous Markov chains. The corresponding transition probability matrices can be computed analytically.
- The stationary probability $P\{\boldsymbol{z}_v(k) = 1\}$ can also be computed analytically.

Key Observation: In most cases, the need for more than 2 RMU's in a given system configuration can not be justified on the tracking performance criterion alone.

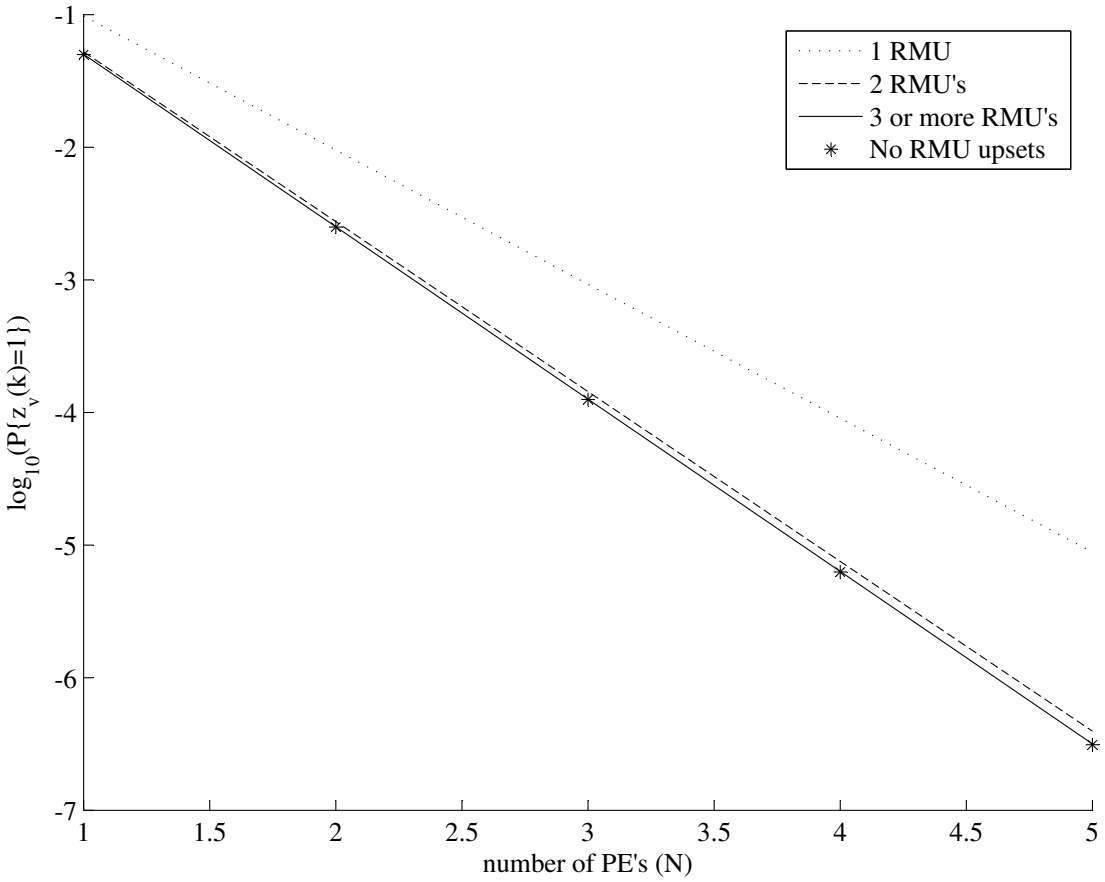

Fig. 3: Theoretically computed $\log_{10}(P\{\boldsymbol{z}_v(k) = 1\})$ versus the number of PE's and as a function of the number of RMU's.

Key Observation: Since the voter output can be approximated as a homogeneous Markov chain, it is possible to compute estimates of J_w analytically using theory for Markov jump-linear systems.

Table 1: Theoretical and simulated (via Monte Carlo methods) values of J_w for two dual PE systems.

# of RMU's	theoretical J_w	simulated J_w
1	7.5139	7.6908
2	1.6977	1.6700

Remark: If the network in the simulator is entirely replaced with a first-order homogeneous Markov chain (i.e., five lines of code), the change in observed tracking performance is negligible!

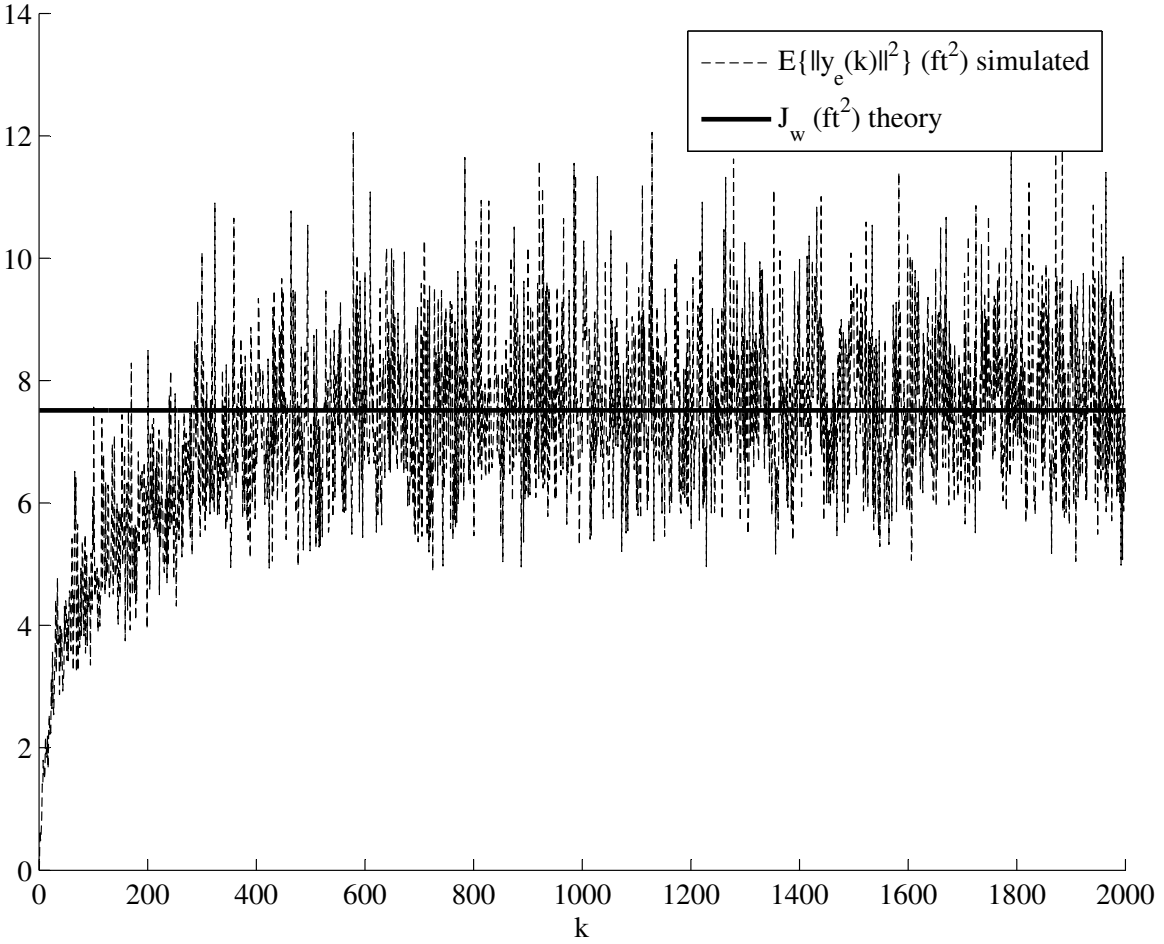

Fig. 4: Simulated tracking error, $E\{\|\boldsymbol{y}_e(k)\|^2\}$, and J_w for a dual PE system with one RMU.

3.2 Fault Injection Experiments

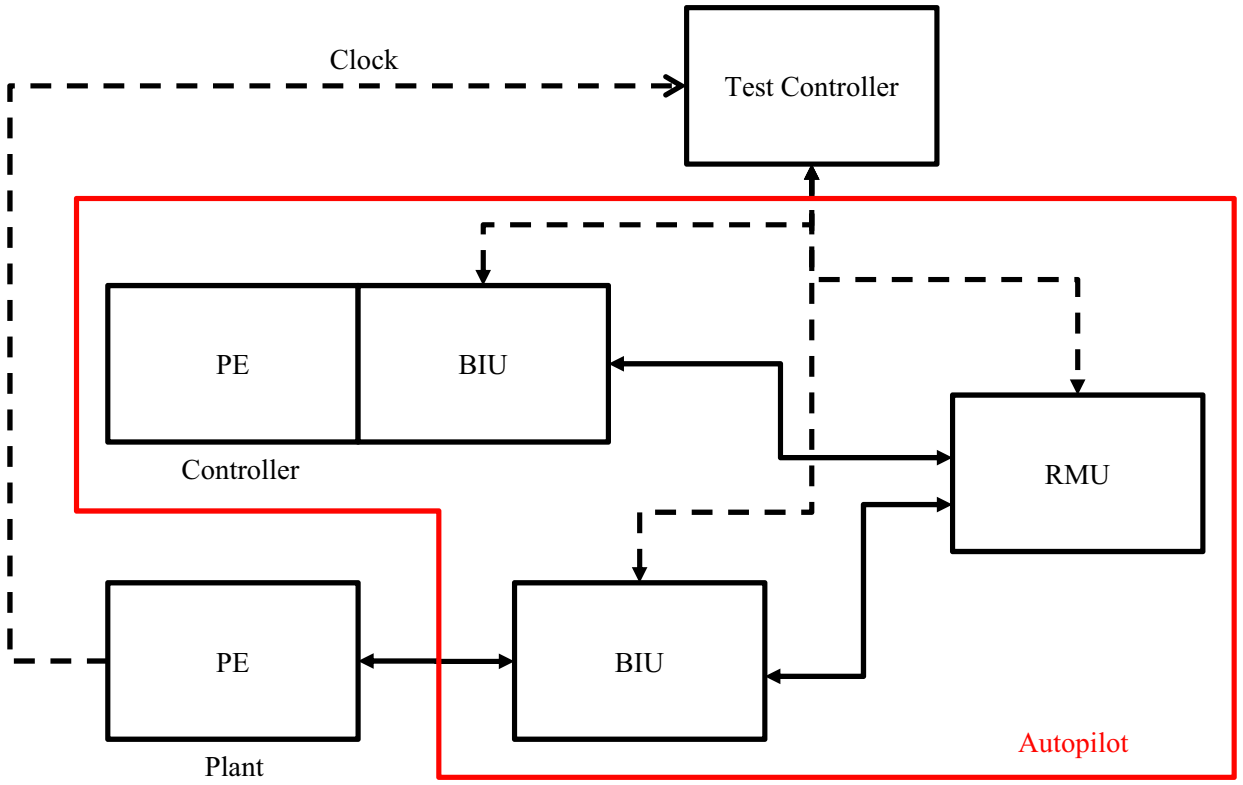

Fig. 5: Conceptual view of a SAFETI Lab simulated fault injection experiment.

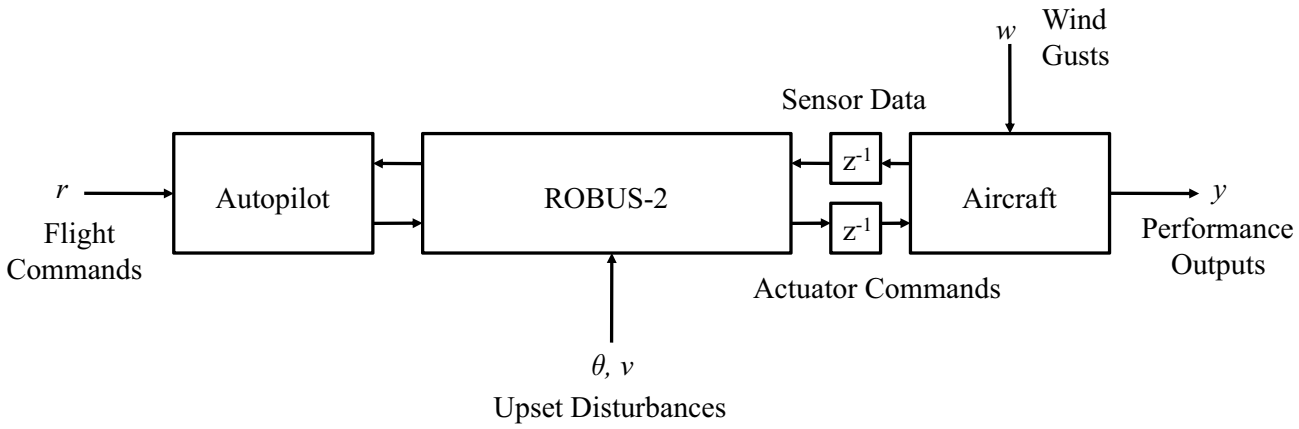

Fig. 6: Closed-loop flight simulator using measured upset disturbances.

Methodology:

- Plant and controller PE's will not run dynamical simulation software, but only emulate the transmission of data packets.
- Test controller will enforce the fail-silent fault injection assumption.
- Use *FLTLAB 747* simulator to integrate off-line the measured communication system model, the autopilot and the Boeing 747.

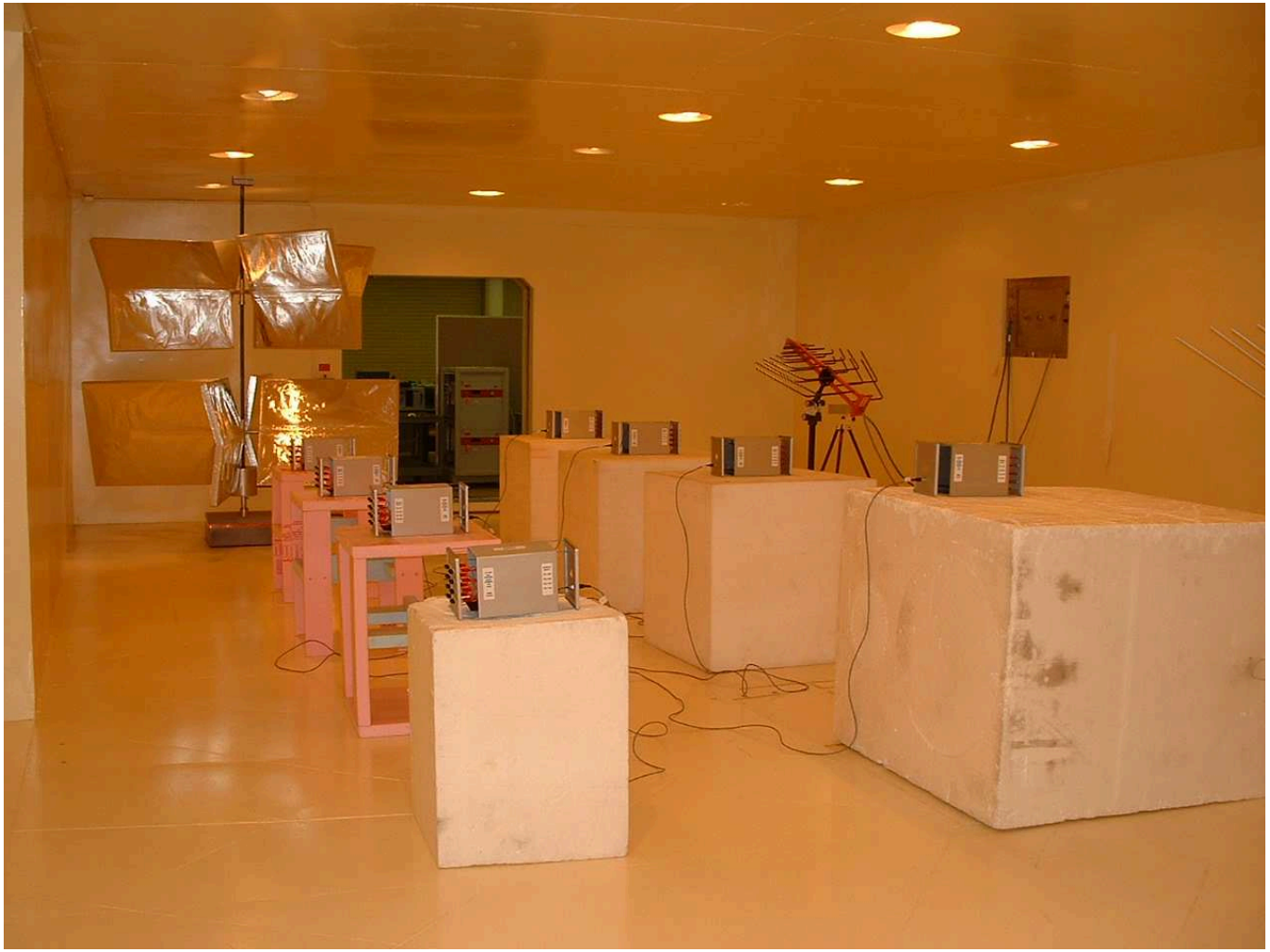

Fig. 7: Year 3 (2009) HIRF test of distributed control system.

Fig. 8: Year 4 (2010) Los Alamos neutron test of distributed control system.

Publications Supported

1. L. A. Duffaut Espinosa, W. S. Gray, and O. R. González, 'On the Bilinearity of Cascaded Bilinear Systems,' *Proc. 46th IEEE Conference on Decision and Control*, New Orleans, Louisiana, 2007, pp. 5581-5587.
2. A. Tejada, O. R. González, and W. S. Gray, 'Stability Analysis of Hybrid Jump Linear Systems with Markov Inputs,' *Proc. 46th IEEE Conference on Decision and Control*, New Orleans, Louisiana, 2007, pp. 6280-6285.
3. H. Herencia-Zapana, O. R. González, and W. S. Gray, 'Dynamically Colored Petri Net Representation of Nonlinear Sample-Data Systems with Embedded Recovery Algorithms,' *Proc. 46th IEEE Conference on Decision and Control*, New Orleans, Louisiana, 2007, pp. 97-102.
4. L. A. Duffaut Espinosa, Racionalidad de la Composición de Funcionales de Entrada/Salida Alimentada por un Proceso Wiener, M.S. Thesis, Pontificia Universidad Católica del Perú, Lima, Perú, 2007.
5. J. R. Chávez-Fuentes, O. R. González, and W. S. Gray 'Towards a Metric for the Assessment of Safety Critical Control Systems,' *Proc. 2008 AIAA Guidance, Navigation and Control Conference*, Honolulu, Hawaii, 2008, Paper AIAA 2008-6804 (invited).

6. W. S. Gray, R. Wang, and O. R. González, 'A Performance Model for a Distributed Flight Control System Subject to Random Upsets,' *Proc. 2008 IEEE Conference on Control Applications*, San Antonio, Texas, 2008, pp. 918-923.

7. A. Tejada, H. Herencia-Zapana, O. R. González, and W. S. Gray, 'Mean Square Stability Analysis of Sampled-Data Supervisor Control Systems,' *Proc. IEEE Conference on Control Applications*, San Antonio, Texas, 2008, pp. 37-42.

8. J. R. Chávez-Fuentes, O. R. González, and W. S. Gray, 'Transformations of Markov Processes in Fault Tolerant Interconnected Systems,' *Proc. IEEE Conference on Control Applications*, Late News Paper, San Antonio, Texas, 2008.

9. A. Tejada, O. R. González, and W. S. Gray, 'Stability of Digital Control Systems Implemented in Error-Recoverable Computers,' *International Journal of Control*, vol. 81, no. 11, November 2008, pp. 1665-1681.

10. W. S. Gray, H. Herencia-Zapana, L. A. Duffaut Espinosa, and O. R. González, 'On Cascades of Bilinear Systems and Generating Series of Weighted Petri Nets,' *Proc. 47th IEEE Conference on Decision and Control*, Cancun, Mexico, 2008, to appear.

11. H. Herencia-Zapana, 'Modeling and Stability Analysis of Nonlinear Sampled-Data Systems with Embedded Recovery Algorithms,' Doctoral Dissertation, Old Dominion University, December 2008.

12. W. S. Gray, H. Herencia-Zapana, L. A. Duffaut Espinosa, and O. R. González, 'Interconnections of Bilinear Systems and Generating Series of Weighted Petri Nets,' *Systems and Control Letters*, under review.

13. L. A. Duffaut Espinosa, W. S. Gray, and O. R. González, 'Growth Bounds for Iterated Integrals with Itô Process Inputs,' *Proc. 41st IEEE Southeastern Symposium on System Theory*, Tullahoma, Tennessee, 2009, under review.

14. J. R. Chávez-Fuentes, O. R. González, and W. S. Gray, 'Transformations of Markov Processes in Fault Tolerant Interconnected Systems,' *Proc. 2009 American Control Conference*, St. Louis, Missouri, 2009, under review.